(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09106456 A**

(43) Date of publication of application: **22.04.97**

(51) Int. Cl **G06T 7/00**

(21) Application number: **07264315**

(22) Date of filing: **12.10.95**

(71) Applicant: **NIPPON DERUMO KK**

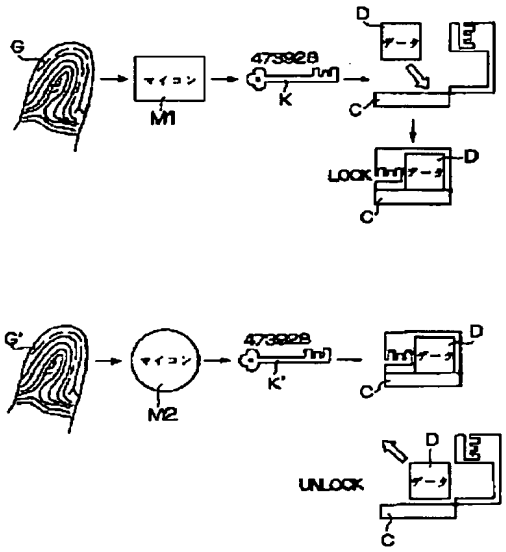
(72) Inventor: **OKI SHINJI**

(54) PERSONAL IDENTIFICATION METHOD IN CARD UTILIZATION, PERSONAL IDENTIFICATION SYSTEM USING IC CARD AND IC CARD USED FOR THE SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To attain perfect personal identification by executing personal identification by collating a user's finger print code generated from the finger print pattern of the card user to the person's finger print code.

SOLUTION: The finger print pattern G of a true possessor is read by an optical reader such as CCD and the person's finger print K is generated through the use of a microcomputer M1. Then data D is stored in the card C and then electronic-sealed (locked) by setting the person's finger print code K as a key. Then the finger print pattern G of the user is read by the optical reader to generate the user's finger print code K' through the use of a microcomputer M2 and to collate this user's finger print code K' to the person's finger print code K to inspect the coincidence of both codes K and K'. Then both finger print code K and K' coincide with each other, the present card user is judged to be a true possessor.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－106456

(43)公開日　平成９年(1997)４月22日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｔ　7/00			Ｇ０６Ｆ　15/62	４６０

審査請求　有　　請求項の数６　ＯＬ　（全　８　頁）

(21)出願番号　特願平7－264315

(22)出願日　平成７年(1995)10月12日

(71)出願人　596108058
日本デルモ株式会社
大阪府松原市南新町１丁目12番25－101号

(72)発明者　大木　信二
大阪府松原市南新町１丁目12番25－609号

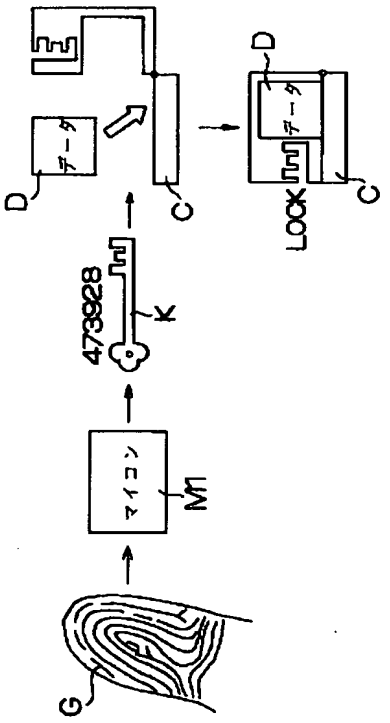
(74)代理人　弁理士　柳野　隆生

(54)【発明の名称】　カード利用における本人確認方法及びＩＣカードを用いた本人確認システム並びに当該システムに用いるＩＣカード

(57)【要約】

【課題】　機密保護がほぼ完璧であり、磁気カード、ＩＣカード及び光ＩＣカードの全てに適用でき、しかも機密保護のために消費する記憶容量も極めて少なく、カードに要求される仕様も従来とほぼ同等の水準間に合うカード利用における本人確認方法を提供せんとするものである。

【解決手段】　真正所持者の指紋パターンから一定のアルゴリズムに従って再現確定性を有して造成される本人指紋コードをカード発行時にカードに登録しておき、カード使用時にカード使用者の指紋パターンから前記アルゴリズムと同じアルゴリズムに従って使用者指紋コードを造成し、この使用者指紋コードを前記本人指紋コードと照合することにより本人確認を行うことを特徴としている。



1

【特許請求の範囲】

【請求項１】　カード使用時に、カードに登録されている特定コードと同じコードを使用することにより本人確認を行うカード利用における本人確認方法において、
カードを発行する際には、
真正所持者の指紋パターンを読み取り、読み取った指紋パターンに基づいて、同じ指紋であれば常に同じコードが再現される再現確定性が保証されたアルゴリズムにしたがって、そのコード長を他のデータの格納領域を圧迫しない範囲に制限した特定コードを造成して、この特定コードを本人指紋コードとしてカード内に登録しておき、
カードを使用する際には、
使用者の指紋パターンを読み取り、本人指紋コードを造成したときと同じアルゴリズムに基づいてカード使用者の指紋パターンから特定コードを造成してこれを使用者指紋コードとして特定するとともに、この使用者指紋コードをカード内に登録された本人指紋コードと照合することによりカード使用者が真正所持者であるか否かを判断してなるカード利用における本人確認方法。

【請求項２】　メモリ回路を搭載したＩＣカードと、
真正所持者の指紋パターンを読み取る指紋読取部を有し、この指紋パターンから同じ指紋であれば常に同じコードが再現される再現確定性が保証されたアルゴリズムにしたがって、そのコード長が他のデータの格納領域を圧迫しない範囲に制限された本人指紋コードを造成する本人指紋コード造成手段と、
造成された本人指紋コードをＩＣカードに登録する手段と、
カード発行時にカード使用者の指紋パターンを読み取る指紋読取部を有し、本人指紋コードを造成したときと同じアルゴリズムに基づいてカード使用者の指紋パターンから使用者指紋コードを造成する使用者指紋コード造成手段と、
使用者指紋コードと本人指紋コードとを照合してカード使用者が真正所持者であるか否かを判断する照合手段と、
を備えたＩＣカードを用いた本人確認システム。

【請求項３】　本人指紋コード造成手段と使用者指紋コード造成手段を同じ装置で共用してなる請求項２記載のＩＣカードを用いた本人確認システム。

【請求項４】　本人指紋コード造成手段、使用者指紋コード造成手段のうち指紋読取部を除く他の部分と照合手段をＩＣカード内部のＣＰＵとメモリにより構成した請求項２又は３記載のＩＣカードを用いた本人確認システム。

【請求項５】　本人指紋コード造成手段、使用者指紋コード造成手段のうち指紋読取部を除く他の部分と照合手段を汎用パソコン内部のＣＰＵとメモリにより構成した請求項２又は３記載のＩＣカードを用いた本人確認システム。

2

【請求項６】　取引内容やプライバシー情報を記憶するデータ収容部と、
同じ指紋であれば常に同じコードが再現される再現確定性が保証されたアルゴリズムにしたがって真正所持者の指紋パターンから造成され且つそのコード長が他のデータの格納領域を圧迫しない範囲に制限した本人指紋コードを前記データ収容部内のデータを封印する鍵として登録する本人指紋コード登録部と、
を有するＩＣカード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はカード利用における本人確認方法とこの方法を用いたＩＣカードの運用システム並びにこのシステムに用いるＩＣカードに関する。

【０００２】

【従来の技術】現代社会には多くのカードが流通しているが、これらカードには通常、本人確認用の情報が登録されている。本人確認用情報の登録形態の最も古典的なものとしてはプラスチックカードに登録番号を可視的に打刻したものがあるが、より重要度の高いデータを取り扱うカードでは電気的、磁気的あるいは光学的方法により本人確認情報となる暗証番号を不可視な状態で登録している。電気的に登録するものの代表としてはＩＣカードがあり、磁気的に登録するものとしては現行のキャッシュカードやクレジットカードに利用されている磁気カードがあり、また光学的に登録するものとしては光ＩＣカードがある。

【０００３】

【発明が解決しようとする課題】ところで、ＩＣカード、磁気カードや光ＩＣカード等では、カード使用時の本人確認は、テンキー等を用いて端末装置に打ち込んだ暗証番号をカード内に登録された暗証番号（以下、カード内暗証番号と称す）と照合することにより行っている。しかしながらこの技術はカード内暗証番号が第三者に知られないことを前提にした技術であるため、何らかの方法でカード内暗証番号が第三者に知られてしまうとカードが不正使用されてしまう。カード内暗証番号はカード保有者の不注意によっても漏れるし、カード自体を解析することによっても解読することができる。特に磁気カードはその分野の技術を有するものであれば暗証番号の取得はそれほど困難ではない。一方ＩＣカードや光ＩＣカードは解析により高度な技術を必要とするものの、それでも解析自体が完全に不可能というわけではなくセキュリティー上の問題は完全には払拭されていない。

【０００４】このようなセキュリティー上の不安を抱えながらも近年、カードの利用分野は飛躍的に拡大しつつある。例えばキャッシュカードやクレジットカードは勿論のこと、個人の健康、病歴を管理する医療カード、身

分等を証明するＩＤカード、更には住民票、家族構成、所得、納税状況を一元管理する市民カード等の構想もあり、その重要性は著しく増している。最近にいたっては通信回線上での電子取引における代金決済の手段としても前記各カード、中でも特にＩＣカードの利用が検討されつつあり、このような現状からカード利用においてカードの不正使用を完全に防止できるより確実な本人確認方法の確立が急がれている。

【０００５】本発明はかかる現況に鑑みてなされたものであり、カードの不正使用をほぼ完璧に防止でき、且つ磁気カード、ＩＣカード及び光ＩＣカードの全てに応用でき、しかもカード自体に要求される仕様（スペック）も従来とほぼ同等のもので充分間に合う本人確認方法を提供せんとするものである。

【０００６】

【課題を解決するための手段】カードの不正使用をなくすために真先に考えられるのはカード内暗証番号の格納方法の工夫や暗証番号の複雑化あるいは暗号化である。しかしながらこれら方法は磁気カードには適用しにくく汎用性に欠ける。またこれら工夫を行ったとしても、カード内暗証番号の解読を完全に防止することはできない。

【０００７】そこで本発明者は、カード内暗証番号はいかに工夫をしても原理的には解読される可能性があるとの観点に立ち、仮にカード内暗証番号が解読されたとしても不正使用を禁じることができる本人確認方法について検討した。その結果、「指紋」が本人確認用情報として利用できるとの着想を得た。しかしながら、指紋パターンをそのままカード内に記録すると多くの記憶容量が必要となり、本来活用すべき他の管理データの格納領域が圧迫されるという問題がある。更に磁気カードにいたってはその記憶容量が少ないために指紋パターンの登録自体が不可能であるという問題がある。

【０００８】本発明者はこのような問題を解決する方法として、指紋パターンをそのまま登録するのではなく、指紋パターンに基づいてコード長を他のデータの格納領域を圧迫しない範囲に制限した特定コードを造成し、この特定コードを指紋パターンに代えて登録することを着想した。このような着想に基づいて完成された本発明は次の内容を有する。

【０００９】請求項１記載の発明は、カード使用時に、カードに登録されている特定コードと同じコードを使用することにより本人確認を行うカード利用における本人確認方法において、カードを発行する際には、真正所持者の指紋パターンを読み取り、読み取った指紋パターンに基づいて、同じ指紋であれば常に同じコードが再現される再現確定性が保証されたアルゴリズムにしたがって、そのコード長を他のデータの格納領域を圧迫しない範囲に制限した特定コードを造成して、この特定コードを本人指紋コードとしてカード内に登録しておき、カードを使用する際には、使用者の指紋パターンを読み取り、本人指紋コードを造成したときと同じアルゴリズムに基づいてカード使用者の指紋パターンから特定コードを造成してこれを使用者指紋コードとして特定するとともに、この使用者指紋コードをカード内に登録された本人指紋コードと照合することによりカード使用者が真正所持者であるか否かを判断することを特徴としている。

【００１０】また前記方法を実現するＩＣカードを用いた本人確認システムである請求項２記載の発明は、メモリ回路を搭載したＩＣカードと、真正所持者の指紋パターンを読み取る指紋読取部を有し、この指紋パターンから同じ指紋であれば常に同じコードが再現される再現確定性が保証されたアルゴリズムにしたがって、そのコード長が他のデータの格納領域を圧迫しない範囲に制限された本人指紋コードを造成する本人指紋コード造成手段と、造成された本人指紋コードをＩＣカードに登録する手段と、カード発行時にカード使用者の指紋パターンを読み取る指紋読取部を有し、本人指紋コードを造成したときと同じアルゴリズムに基づいてカード使用者の指紋パターンから使用者指紋コードを造成する使用者指紋コード造成手段と、使用者指紋コードと本人指紋コードとを照合してカード使用者が真正所持者であるか否かを判断する照合手段と、を備えたことを特徴としている。

【００１１】本人指紋コード造成手段と使用者指紋コード造成手段は同一装置で共用することができる。

【００１２】本人指紋コード造成手段、使用者指紋コード造成手段のうち指紋読取部を除く他の部分と照合手段はＩＣカード内部のＣＰＵとメモリにより構成しても良いし、あるいは汎用パソコン内部のＣＰＵとメモリにより構成してもよい。

【００１３】このようなシステムに使用されるＩＣカードを規定した請求項６記載の発明は、取引内容やプライバシー情報を記憶するデータ収容部と、同じ指紋であれば常に同じコードが再現される再現確定性が保証されたアルゴリズムにしたがって真正所持者の指紋パターンから造成され且つそのコード長が他のデータの格納領域を圧迫しない範囲に制限した本人指紋コードを前記データ収容部内のデータを封印する鍵として登録する本人指紋コード登録部と、を有することを特徴としている。

【００１４】

【発明の実施の態様】次に本発明の詳細を図面に基づき説明する。図１はカード発行時の処理内容、図２はカード使用時の処理内容を示している。ここではカードとしてＩＣカードを用いた場合について述べる。

＜カード発行時の処理＞先ず真正所持者の指紋パターンＧを、例えばＣＣＤ等の光学読取装置によって読み取り、マイクロコンピュータ（以下、マイコンと称す）Ｍ１を用いて本人指紋コードＫを造成し、カードＣ内にデータＤを格納したうえ本人指紋コードＫを鍵として電子的に封印（施錠）する。データＤとしては、姓名、住

所、電話番号等の基礎データを始めとして各種取引データなどがある。指紋パターンＧから指紋コードＫを造成するアルゴリズムは常に同じものが用いられる。このアルゴリズムは公開することが原則であるが非公開とすることもできる。指紋コード造成作業を実行するマイコンＭ１はカードＣがＣＰＵ非搭載のメモリカードである場合にはカードＣ外に設けるが、カードＣがＣＰＵ搭載型のＩＣカードである場合にはカードＣ内ＣＰＵを指紋コード造成用マイコンＭ１として利用することができる。セキュリティーを高める観点からはカードＣ内ＣＰＵを指紋コード造成用マイコンとして使用することが好ましい。カードＣ外に指紋コード造成用マイコンＭ１を設ける場合、指紋コード造成用マイコンＭ１はボード化してパーソナルコンピュータ（以下、パソコンと称す）の拡張スロットに装着したり、あるいはパソコン本体に搭載されているＣＰＵ及びメモリをソフトウェア上で制御して指紋コード造成用マイコンとして使用することができる。マイコンによって造成される指紋コードは、同じ指紋であれば常に同じコードが再現される再現確定性を保証されている必要である。また指紋コードのコード長は他のデータ領域を圧迫しない範囲とし、通常５桁～１０桁程度とする。本人指紋コードＫは唯一無二のものである必要はなく、その桁数は少なくても実用上問題はない。本人指紋コードは数字のみから構成してもよいし、また英文字やその他記号等を含んでいてもよい。指紋パターンから指紋コードを造成するアルゴリズムとしては種々のものが考えられるが、例えば図３に示すように指紋パターンを複数エリアに分割し、それぞれのエリア内を横切る隆線の密度を数値に置き換えて得られた数値群を基にして造成すること、あるいは隆線の断端、分岐、三角州形成、短棒状あるいは点状隆線、屈曲等、指紋の特徴部分に着目して数値化すること等が採用可能である。尚、指紋の読み取り位置や読み取り角度の相違が造成される指紋コードに影響を与えないようにするために、読み取った指紋パターンはメモリー上で定位置に移動させたのち指紋コードを造成することが望まれる。

【００１５】＜カード使用時の処理＞カード使用者の指紋パターンＧ’を光学読取装置等によって読み取り、マイコンＭ２を用いて使用者指紋コードＫ’を造成するとともに、この使用者指紋コードＫ’をカードＣ内に登録された前記本人指紋コードＫと照合し、両コードＫ，，Ｋ’の一致性を検証する。カード使用者がカードの真正所持者である場合、使用者指紋パターンＧ’は本人指紋パターンＧと同じであるから両指紋パターンＧ，Ｇ’から造成される指紋コードＫ，Ｋ’は当然一致する。指紋コードＫ，Ｋ’が一致したときには現在のカード使用者を真正所持者であると判断する。一致性を判断する照合部はカードＣ内部に設けることもカードＣ外部に設けることもできる。指紋コードＫ，Ｋ’が一致すれば、プロテクトを解除（解錠）してカード内データやホストコンピュータへのアクセスを許可する。尚、カードが磁気カードであってカード内に取引内容等のデータ記録部を持たないものである場合には、カード内データへのアクセスを行うことなくホストコンピュータにアクセスする。使用者指紋コードＫ’を造成する際のアルゴリズムは本人指紋コードＫを作成する際のアルゴリズムと全く同じものである。本人指紋コードＫを造成したマイコンＭ１と使用者指紋コードＨ’を造成するマイコンＭ２とは通常異なるが、指紋コードを造成するアルゴリズムが同一であるため、造成される指紋コードの再現確定性は保証される。本人指紋コードＫと使用者指紋コードＫ’との一致性の判断は、全桁完全一致が原則であるが、光学読取装置の機器誤差等を考慮して許容範囲を設定して多少基準を甘くする場合もある。

【００１６】このような本人確認方法は例えば、カードを用いた各種取引における本人照会に使用することができる。各種取引とは預貯金の引き出し、クレジットカードによる商品購入、パソコン通信における電子取引等における代金決済であり、これら以外にも数多くのものがある。各種取引に用いるカードとしてはＩＣカードが主たる対象となるが、光ＩＣカードや磁気カードも除外するものではない。以下の説明ではＩＣカードを例にして話を進める。

【００１７】カード発行時に行う指紋コードの登録やカード使用時に行う指紋コードの照合には例えば図４で示されるような指紋コード照合・登録装置１を用いることができる。指紋コード照合・登録装置１は指紋読取部２とカード読み書き部３を一つのケース内に一体化した構成である。指紋読取部２はＣＣＤ等の光学読み取り装置を用いることが最も現実的であるが、指紋パターンを読み取れるものであれば他のセンサを用いてもよい。指紋コード照合・登録装置１は指紋コード造成と使用者指紋コードと本人指紋コードとの一致性を検証する照合手段の全てを内蔵させた独立装置としてもよいが図５に示すように、汎用パソコンＰを接続する等して前記各手段のうちＣＣＤ以外の部分は汎用パソコンＰのＣＰＵやメモリによって構成してもよい。指紋コード照合・登録装置１は銀行や商店に設置したり、あるいは小型且つ簡易なものを開発すればパソコン通信の端末機に接続したりすることもできる。

【００１８】カード読み書き部３はカード装着口３ａを有し、その内奥にデータ授受部３ｂを設けた構成である。データ授受の方式は有接点アクセス方式でも良いが、磁気誘導又は静電誘導等の原理を応用した無接点アクセス方式を採用することが好ましい。無接点アクセス方式であれば、カード表面に接触端子が露出しないので、端子汚損によるデータエラーの発生がなくカードの取扱い性が飛躍的に向上する。また磁気誘導又は静電誘導によって供給された電力をカード内に組み込んだ二次電池に充電するようにすればカードを完全密封すること

が可能となり、カードに高度な耐水性を与えることができる。またＩＣカード内のメモリにフラッシュメモリ等の不揮発メモリを用いた場合は、記憶内容保持のための電力は不要となるので、ＩＣカード内に電池を収容する必要はない。

【００１９】ＩＣカードＣとしてはメモリ回路を主体としたものが用いられる。ＩＣカードＣはＣＰＵ搭載型とＣＰＵ非搭載型のいずれを用いることもできる。ＣＰＵ搭載型の場合、ＩＣカードＣの演算機能を利用して指紋コード造成作業や、造成された指紋コードとカード内に登録された本人指紋コードを照合する作業の全てをカード内で処理完結させることができるので、セキュリティーは一層高まる。

【００２０】図６は本人指紋コードＫを鍵としてカード内のデータＤを封印した様子を概念的に示している。メモリ回路は同一構造のメモリ素子を集積して構成されるものでソフトウェア上でデータ収容部ｄとこれを封印（施錠）する鍵部ｋとに区分している。鍵部ｋとデータ収容部ｄの配分は適宜設定できる。図６として示したものはカード内に設けた単一のデータ収容部ｄ内のデータＤを単一の鍵Ｋで封印（施錠）した場合であるが、他の態様も適宜採用できる。例えば単一のデータ収容部を二種以上の鍵で封印（施錠）することや、図７に示すようにカード内のメモリをソフトウェア上で複数領域に区分し、それぞれの領域内に設けたデータ収容部ｄａ，ｄｂ，……に対してそれぞれ別の鍵Ａ，Ｂ，……を設けることもできる。これら複数の鍵を設ける場合、最も重要度の高いデータへのアクセスを許可する鍵にのみ指紋コードを用いることとし、他の重要度の低いデータへのアクセスについては従来よりキャッシュカードに採用されているような単なる暗証番号を用いることなどが考えられる。

【００２１】カードに登録する指紋コードは指紋パターンから造成するものであってキーボードから入力するものではないから、手入力可能であるか否かを基準にして桁数を制限する必要はない。しかしながら、あまり桁数が多いとデータ収容部として確保できるメモリ量が減る。指紋パターンのコード長はこれらのことを考慮して決定する。指紋コードは唯一無二のものである必要はなく、その桁数は少なくても実用上問題はない。本発明はカード使用時に使用者の指紋パターンから造成した使用者指紋コードをカード内部に登録された本人指紋コードと照合するものであるから、仮に異なった指紋パターンから同じ指紋コードが造成されるような場合があったとしても、その頻度が極めて稀であるならば実用上問題はない。いかに高度な技術を持った者であっても、真正所持者の本人指紋コードと同じ指紋コードが造成されるように自分の指紋を変造することは不可能である。これは、指紋コードを公開しておいても問題がないことを意味している。またこれは指紋コードを認証する公的あるいは私的な証明機関の設立が可能であることも意味し、現在の印鑑証明発行業務的な役割をこの証明機関が担えることも意味している。指紋コードを非公開とした場合には、取引の種類によっては使用者指紋パターンからの使用者指紋コードの造成することなく指紋コードを手入力することも可能である。この場合の指紋コードの手入力行為は従来のキャッシュカードにおける暗証コードの入力に相当し、重要度が低い簡易な取引のみに限って、指紋パターンからの指紋コードの造成を行うことなく非公開の指紋コードのみをキーボードから直接入力することで済ますというものである。

【００２２】指紋コードを認証する証明機関を設けた場合は、カードの使用者が間違いなく前記証明機関に届出された特定の人物であることが証明できるので、指紋コードによる本人確認の信頼性は一層確かなものとなる。証明機関への指紋コードの登録は登録者が証明機関に出向き、証明機関に設置された指紋コード照合・登録装置に指紋を読み取らせることで行ってもよいが、登録者が証明機関に出向くことなく行う方法も考えられる。図８はこの方法を示し、図中①～⑥は各段階を示している。以下、各段階を説明する。

①登録希望者が証明機関に指紋コードの登録手続きを申し込む。指紋コードの登録を希望する者は、自分が決めた４桁程度の暗証番号（例えば、２１３１）を添えて、郵便又はパソコン通信で証明機関Ｑに申し込む。

②証明機関Ｑは当該機関が指定した特定の数字（例えば、４５６７）をＩＣカードのメモリに書き込み、この特定数字（４５６７）を登録希望者が指定した暗証番号（２１３１）によって施錠したうえ、ＩＣカードを登録希望者に郵便又は宅配等で送付する。

③ＩＣカードを入手した登録希望者は、自宅のパソコンに接続された指紋コード照合・登録装置１にＩＣカードＣを装着し、自分が指定した暗証番号（２１３１）を用いて解錠し、証明機関Ｑが指定した特定数字（４５６７）を取り出して通信回線を通じて特定数字（４５６７）をこの証明機関Ｑに送る。これを受け取った証明機関Ｑは送られてきた特定数字（４５６７）が当該機関が設定した特定数字（４５６７）と一致しているか否かを照合することにより、交信相手が当該証明機関Ｑが管理している特定の登録希望者であることを認識し、この回線接続中に行われる証明機関Ｑに対する手続が特定個人によるものであることを認識する。特定数字（４５６７）は証明機関Ｑ自身が自己が発行したＩＣカードを特定するためのものであって、登録希望者にとってはその内容を知る意味はないから、特定数字（４５６７）を暗号化処理して登録希望者にわからないようにすることもできる。

④通信回線を開いた状態で、姓名、住所、電話番号、生年月日等の基礎データをカード内メモリに書き込む。

⑤登録希望者は指紋コード照合・登録装置１によって自

分の指紋を読み取って指紋コード（例えば、４７３９２８）を造成し、この段階で仮の鍵であった２１３１を破棄して本人指紋コード（４７３９２８）を正式な鍵とする。これ以降はこの本人指紋コード（４７３９２８）でなければ施錠・解錠はできず、本人指紋コード（４７３９２８）によってカード内部のデータが保護されることになる。

⑥登録希望者は本人指紋コード（４７３９２８）と一緒に姓名、住所、電話番号、生年月日等の基礎データのうち公開しても問題のないデータを証明機関Ｑに送信して登録する。証明機関Ｑには送信したデータが本人指紋コード（４７３９２８）と関連づけられて登録される。本人指紋コード（４７３９２８）は本人指紋から再現確定性を有して造成されるものであるから、本人認証の確度という点では指紋を登録したのと同等の信頼性があり、しかも指紋パターンそのものを登録するものではないからプライバシー上の問題が発生することもない。

【００２３】本願発明は従来より本人確認を必要とする各種手続や各種取引に適用することが可能であることは勿論のこと、今後発展が期待される通信回線上での電子取引にも広く利用できる。通信回線を通じた電子取引の場合、端末機としての各パソコンには指紋コード照合・登録装置の接続又は内蔵が必要となるが、このような装置は量産すれば飛躍的に安価に提供できるうえにその機能の大部分をパソコン本体のＣＰＵによって担わせることもできるから、本システムを普及させるうえでの経済的な障害はまったくない。

【００２４】

【発明の効果】本発明は、真正所持者の指紋パターンから造成された本人指紋コードをカードに登録しておき、カード使用時にカード使用者の指紋パターンから造成される使用者指紋コードを前記本人指紋コードと照合して本人確認を行うものであるから、第三者が本人になりすますことは原理的に不可能であり、ほぼ完璧な本人確認が可能となる。しかも本発明は指紋パターンそのものを登録するものではなく、この指紋パターンから造成される指紋コードを登録するものであるから、指紋コードを登録するために確保すべきカード内の記憶容量はわずかである。したがって本発明はＩＣカードや光ＩＣカードは勿論のこと磁気カードにも適用でき、しかもＩＣカードや光ＩＣカードに適用した場合はメモリのほとんどを取引データやプライバシーデータ等を登録する領域として確保することができる。また指紋コードを認証する証明機関を設立して本システムを法的に保証する環境を整備した場合にも、証明機関には指紋パターン自体が登録されるわけではないからプライバシー上の何らの問題も発生せず、しかも登録するためのメモリ容量も少なくて済むから、証明機関の設備上の負担も小さなもので済む。

【図面の簡単な説明】

【図１】　本発明における施錠の考え方を示す説明図

【図２】　本発明における解錠の考え方を示す説明図

【図３】　指紋パターンから指紋コードを造成する方法の一例を示す説明図

【図４】　指紋コード照合・登録装置の一例を示す説明図

【図５】　指紋コード照合・登録装置をパソコンに接続した例を示す説明図

【図６】　カード内メモリをソフトウェア上で鍵部とデータ収容部とに区分し、データ収容部内のデータを鍵で施錠した様子を示す説明図

【図７】　カード内メモリをソフトウェア上で複数の領域に区分してそれぞれの領域内のデータを別個の鍵で施錠した様子を示す説明図

【図８】　指紋コードを証明機関に登録する方法の一例を示す説明図

【符号の説明】

Ｇ　真正所持者の指紋パターン　　Ｇ’カード使用者の指紋パターン

Ｍ１，Ｍ２　マイクロコンピュータ　Ｄ　データ

Ｋ　真正所持者の指紋コード　　Ｋ’カード使用者の指紋コード

Ｃ　カード

１　指紋コード照合・登録装置　　２　指紋読取部

３　カード読み書き部

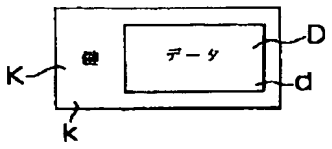
３ａ　カード装着口　　３ｂ　データ授受部

ｄ　データ収容部　　ｋ　鍵部

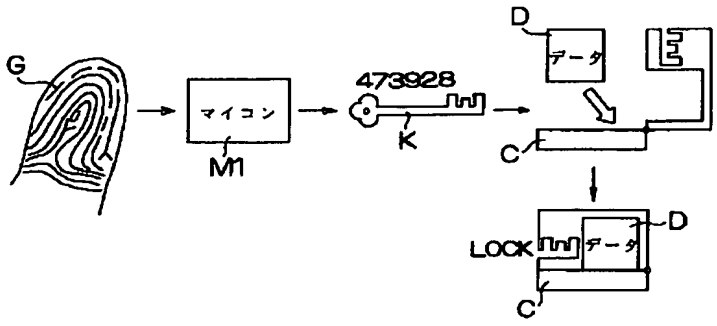
ｄａ～ｄｚ　データ収容部　　Ａ～Ｚ　鍵

Ｑ　証明機関

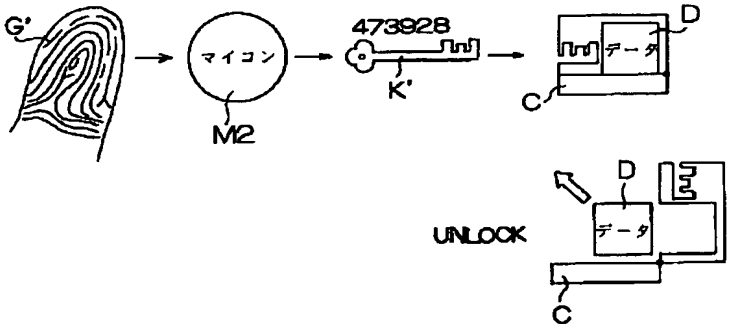
【図６】



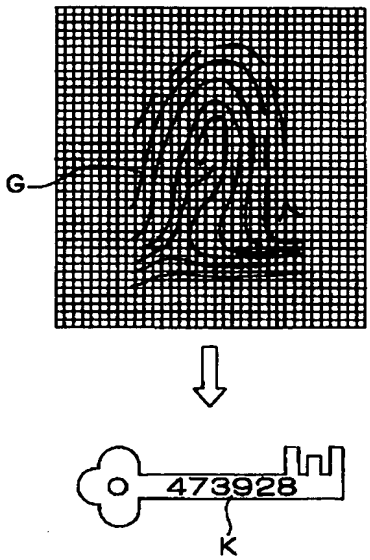
【図１】


G
マイコン
M1
473928
K
D
データ
C
LOCK
D
データ
C

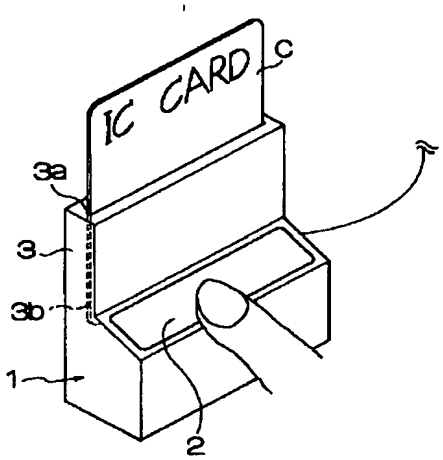
【図２】


G'
マイコン
M2
473928
K'
D
データ
C
UNLOCK
D
データ
C

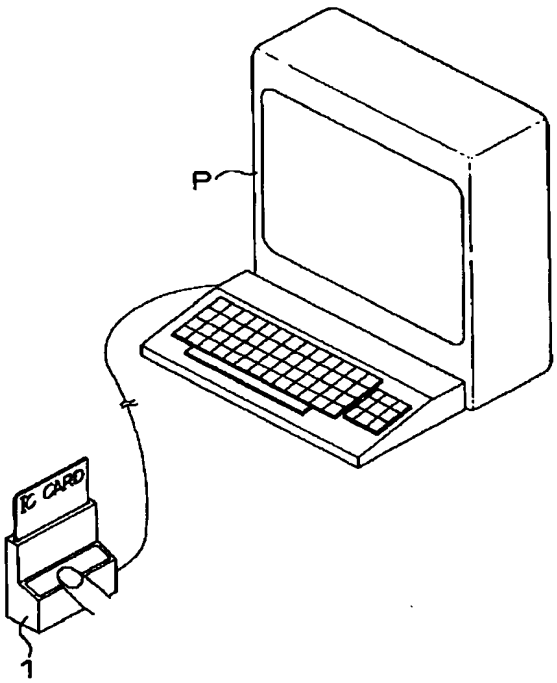
【図３】


G
473928
K

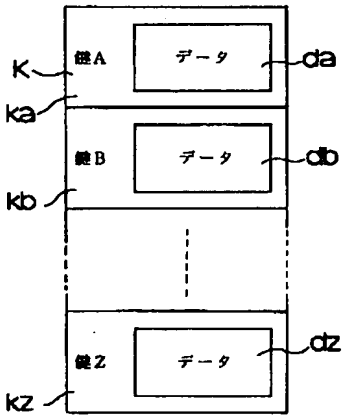
【図４】


IC CARD
C
3a
3
3b
1
2

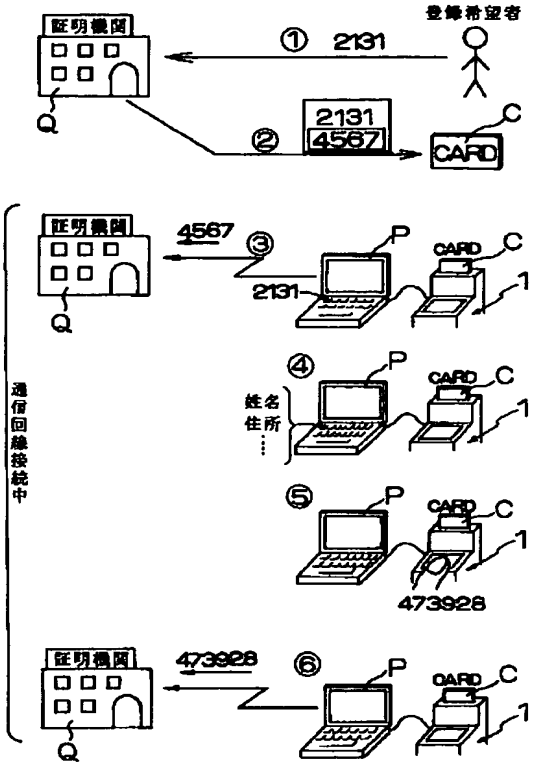
【図５】


P
IC CARD
1

【図７】


K
鍵A
データ
da
ka
鍵B
データ
db
kb
鍵Z
データ
dz
kz

【図８】


証明機関
登録希望者
① 2131
Q
② 2131 4567
C
CARD
通信回線接続中
4567
③
P
CARD
C
1
2131
④
姓名
住所
⑤
473928
⑥